Reconstructing Extended Perfect Binary One-Error-Correcting Codes from Their Minimum Distance Graphs

Ivan Yu. Mogilnykh, Patric R. J. Östergård, Olli Pottonen, Faina I. Solov'eva

Abstract— **The minimum distance graph of a code has the codewords as vertices and edges exactly when the Hamming distance between two codewords equals the minimum distance of the code. A constructive proof for reconstructibility of an extended perfect binary one-error-correcting code from its minimum distance graph is presented. Consequently, inequivalent such codes have nonisomorphic minimum distance graphs. Moreover, it is shown that the automorphism group of a minimum distance graph is isomorphic to that of the corresponding code.**

Index Terms— **minimum distance graph, extended perfect binary code, reconstructibility, weak isometry**

I. Introduction

A binary code of length n is a subset of $\mathbf{F}_2^n$, where $\mathbf{F}_2 = \{0,1\}$ is the field of two elements. Throughout this work, we use "code" in the meaning of "binary code". The *support* $\mathrm{supp}(\mathbf{x})$ of a word $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is the set of its nonzero coordinates, the *weight* $\mathrm{wt}(\mathbf{x})$ of $\mathbf{x}$ is the number of nonzero coordinates, and the *Hamming distance* $d_H(\mathbf{x}, \mathbf{y})$ is the number of coordinates in which the words $\mathbf{x}$ and $\mathbf{y}$ differ. Formally, $\mathrm{supp}(\mathbf{x}) := \{i : x_i = 1\}$, $\mathrm{wt}(\mathbf{x}) := |\mathrm{supp}(\mathbf{x})|$ and $d_H(\mathbf{x}, \mathbf{y}) := \mathrm{wt}(\mathbf{x} - \mathbf{y})$.

The *minimum distance* of a code is the minimum Hamming distance between any pair of distinct codewords. For a code with minimum distance d, the balls of radius $r = \lfloor (d-1)/2 \rfloor$ centered around the codewords are nonintersecting and such a code is called an r*-error-correcting code*. If the balls cover the entire ambient space, the code is called *perfect*, or more specifically, r*-perfect*. With one exception (the binary Golay code), all nontrivial perfect binary codes have $d = 3$, $n = 2^m - 1$.

A permutation π acts on a codeword by permuting the coordinates. A pair $(\pi, \mathbf{z})$ acts on a codeword $\mathbf{x}$ as $(\pi, \mathbf{z})(\mathbf{x}) = \mathbf{z} + \pi(\mathbf{x})$. Two codes are *equivalent* if the action of such a pair on the codewords of one code produces the codewords of the other. The set of all such pairs that map a code onto itself form the *automorphism group* of the code.

A *Steiner system* $S(t, k, v)$ is a set of v *points* together with a collection of *blocks*, each consisting of k points, such that any t points occur in a unique block. The Steiner systems $S(2, 3, v)$ and $S(3, 4, v)$ are called *Steiner triple systems* and *Steiner quadruple systems*, respectively, or $\mathrm{STS}(v)$ and $\mathrm{SQS}(v)$ for short. If C is a 1-perfect code of length n and $\mathbf{x} \in C$, then the blocks $\{\mathrm{supp}(\mathbf{x} - \mathbf{y}) : d_H(\mathbf{x}, \mathbf{y}) = 3,\ \mathbf{y} \in C\}$ form an $\mathrm{STS}(n)$, called the *neighborhood STS* of $\mathbf{x}$. Similarly, if C is an extended 1-perfect code, then each $\mathbf{x} \in C$ has an *neighborhood SQS* with the block set $\{\mathrm{supp}(\mathbf{x} - \mathbf{y}) : d_H(\mathbf{x},\ \mathbf{y}) = 4,\ \mathbf{y} \in C\}$. The *block graph* of an $S(t, k, v)$ has the blocks of the design as vertices, with edges incident to intersecting blocks.

The *minimum distance graph* of a code with minimum distance d has the codewords as vertices and edges between codewords with Hamming distance d. In the rest of the paper we consider such minimum distance graphs. Note that the distance between codewords is then the distance between the corresponding vertices in the graph; this is not to be confused with the Hamming distance.

Phelps and LeVan [1] asked whether 1-perfect codes with isomorphic minimum distance graphs are always equivalent, and this question was answered in the affirmative by Avgustinovich [2], building on earlier work by Avgustinovich and others [3], [4]; in fact, the result was announced already in [3] for lengths $n \geq 31$, but without details.

We start off in Section II by finalizing a proof that extended 1-perfect codes with isomorphic minimum distance graphs are equivalent for $n \geq 256$. The detailed treatment in the rest of the paper makes it possible to handle codes of shorter lengths. We prove in Section III the stronger result that any extended 1-perfect code can be reconstructed from its minimum distance graph, and, in Section IV, show how this implies an analogous result for 1-perfect codes. In Section V we prove that the automorphism groups of these codes are isomorphic to the automorphism groups of their minimum distance graphs for lengths $n \geq 15$. Section VI concludes the paper.

II. Code Isometry and Equivalence

A bijection $I : C_1 \to C_2$ is called an *isometry* if $d_H(\mathbf{x}, \mathbf{y}) = d_H(I(\mathbf{x}), I(\mathbf{y}))$ for all $\mathbf{x}, \mathbf{y} \in C_1$. Moreover, such a mapping is a *weak isometry* if $d_H(\mathbf{x}, \mathbf{y}) = d$ iff $d_H(I(\mathbf{x}), I(\mathbf{y})) = d$, where d is the minimum distance of the codes C_1 and C_2.

We may now rephrase the question by Phelps and LeVan [1] in the defined terms: Are weakly isometric 1-perfect codes always equivalent? The idea of the proof completed in [2] is to combine a proof that weakly isometric such codes are isometric with a proof (from [3], [4]) that isometric such codes are equivalent. We may act analogously for extended 1-perfect codes, and use a result from [5] that isometric such codes are equivalent for lengths $n \geq 256$. Then it only remains to prove that weakly isometric codes are isometric, which can be done for arbitrary lengths.

Theorem 1: Weakly isometric extended 1-perfect codes are isometric.

Proof: We show that one is able to deduce the Hamming distance between any two codewords, given the minimum distance graph. Consider an arbitrary codeword $\mathbf{x}$. The codewords $\mathbf{y}$ with $d_H(\mathbf{x}, \mathbf{y}) = 4$ are given by the minimum distance graph. Having identified all codewords $\mathbf{y}$ with $d_H(\mathbf{x}, \mathbf{y}) \leq i$, we need to distinguish between the cases $d_H(\mathbf{x}, \mathbf{z}) = i+2$ and $d_H(\mathbf{x}, \mathbf{z}) = i + 4$ for a codeword $\mathbf{z}$ in order to proceed with

This work was supported in part by the Graduate School in Electronics, Telecommunication and Automation and by the Academy of Finland, Grant Numbers 107493 and 110196.

I. Yu. Mogilnykh and F. I. Solov'eva are with the Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk, Russia (e-mail: ivmog84@gmail.com, sol@math.nsc.ru).

P. R. J. Östergård and O. Pottonen are with the Department of Communications and Networking, Helsinki University of Technology TKK, P.O. Box 3000, FI-02015 TKK, Finland (e-mail: patric.ostergard@tkk.fi, olli.pottonen@tkk.fi).

induction. If $\mathbf{z}$ has a neighbour $\mathbf{v}$ with $d_H(\mathbf{x},\mathbf{v}) = i-2$, then $d_H(\mathbf{x},\mathbf{z}) = i+2$. All remaining codewords $\mathbf{z}$ with $d_H(\mathbf{x},\mathbf{z}) = i+2$ have $\binom{i+2}{3}$ neighbours that are at Hamming distance i from $\mathbf{x}$, whereas those codewords $\mathbf{z}$ with $d_H(\mathbf{x},\mathbf{z}) = i+4$ have at most $\binom{i+4}{3}/4$ such neighbors (consider respectively the triples and quadruples of $\mathrm{supp}(\mathbf{x}-\mathbf{z})$ in the neighborhood SQS of $\mathbf{z}$). For $i \geq 4$ we have $\binom{i+2}{3} > \binom{i+4}{3}/4$. ■

Theorem 2: Weakly isometric extended 1-perfect codes are equivalent for lengths $n \geq 256$.

Proof: Follows from Theorem 1 and [5]. ■

III. Reconstructing Extended 1-Perfect Codes

A *clique* in a graph is a set of mutually adjacent vertices. The idea of utilizing maximum cliques in reconstruction has earlier been used by Spielman [6]; see also [7]. It follows from a result by Rands [8] that the maximum cliques in the block graph of a Steiner system can be used to identify the points of the design whenever the number of points (v) exceeds a certain value that depends only on the parameters k and t. Unfortunately, the bound derived in [8] for the threshold value is too large for the smallest cases that we want to handle, so we need to carry out a more detailed treatment.

In the preparation for a reconstructibility proof for extended 1-perfect codes, Theorem 3, we prove three lemmata.

Lemma 1: The codewords with Hamming distance 6 can be recognized from the minimum distance graph of an extended 1-perfect code.

Proof: Follows from the proof of Theorem 1. ■

Lemma 2: If Q is a clique in the block graph of an $\mathrm{SQS}(v)$, $v \geq 16$, such that there is no point that occurs in every block of Q, then $|Q| < (v-1)(v-2)/6$.

Proof: Consider a clique Q such that no point occurs in every block of Q. First note that any pair of points is contained in (v-2)/2 blocks of an SQS(v) and therefore in at most (v-2)/2 blocks of Q.

We consider the size of a nonempty Q in three separate cases.

1) There is a point x that occurs in every block of Q except one:
Assume that $x \notin \{a,b,c,d\} \in Q$. Since Q is a clique in the block graph, every block of Q containing x contains at least one of the pairs $\{x,a\},\{x,b\},\{x,c\},\{x,d\}$. From the fact that each pair occurs in at most $(v-2)/2$ blocks, it follows that $|Q| \leq 4(v-2)/2+1 = 2v-3$.

2) There is a pair of points $\{x,y\}$ that intersects every block of Q, but no point occurs in $|Q|-1$ blocks:
There are at least two blocks that do not contain x; let B_1 and B_2 be two such blocks. Since $x \notin B_1$ and $x \notin B_2$, by the assumption $y \in B_1 \cap B_2$. If $|B_1 \cap B_2| = 2$, $B_1 = \{y,a,b,c\}$ and $B_2 = \{y,a,d,e\}$ with distinct elements a,b,c,d,e. Any block that contains x but not y must contain either a (there are at most $(v-2)/2$ such blocks), or b and d (at most 1), or b and e (at most 1), or c and d (at most 1), or c and e (at most 1), so there are at most $(v-2)/2+4$ blocks that contain x but not y. On the other hand, if $|B_1 \cap B_2| = 1$, then $B_1 = \{y,a,b,c\}$ and $B_2 = \{y,d,e,f\}$, and we get at most 9 blocks containing x and intersecting B_1 and B_2, one for each pair with one element taken from $\{a,b,c\}$ and the other from $\{d,e,f\}$. An upper bound for the number of blocks containing x but not y is then $\max\{9, v/2+3\} = v/2+3$ as $v \geq 16$.
By the same argument there are at most $v/2+3$ blocks that contain y but not x. Finally, at most $(v-2)/2$ blocks contain both x and y, so $|Q| \leq (v-2)/2+2(v/2+3) = 3v/2+5$.

3) For every pair of points there is a block of Q that does not intersect the pair:
(Note that in this case no point occurs in $|Q|-1$ blocks). Any pair of points may occur in at most 4 blocks of Q, since Q contains a block B that does not intersect the pair, and each block that contains the pair also contains a point of B.
Take any point x. There are at least two blocks that do not contain x. If these blocks intersect in two points, say $B_1 = \{a,b,c,d\}$ and $B_2 = \{a,b,e,f\}$, we get that each block containing x must contain a (at most 4 blocks), b (at most 4), c and e (at most 1), c and f (at most 1), d and e (at most 1), or d and f (at most 1), giving a total of at most 12 blocks. Similarly, for the situation with one point in the intersection, $B_1 = \{a,b,c,d\}$, $B_2 = \{a,e,f,g\}$, we get an upper bound of $4+3^2 = 13$ blocks. Thus any point occurs in at most 13 blocks.
If each point occurs in at most 8 blocks, we have $|Q| \leq 1+4(8-1) = 29$ as any block must intersect a given block. Assuming that there is a point x occurring in at least 9 blocks, and considering blocks containing x and intersecting a block B that does not contain x, we get by the pigeonhole principle that some pair $\{x,y\}$ with $y \in B$ must occur it at least 3 blocks. Now consider a block $\{x,y,a,b\} \in Q$. There are at most $2 \cdot 13 - 3 = 23$ blocks that intersect $\{x,y\}$. By considering blocks intersecting three blocks $\{x,y,a,b\}$, $\{x,y,c,d\}$, and $\{x,y,e,f\}$, one obtains that a block that does not intersect $\{x,y\}$ must contain one of $2^3 = 8$ sets, $\{a,c,e\}$, etc. Moreover, since no two blocks may intersect in three points, their total number is at most 8. Summing up the number of blocks that intersect $\{x,y\}$ and those that do not, we get that $|Q| \leq 23+8 = 31$.

Combining the results above, we conclude that $|Q| \leq \max(2v-3, 3v/2+5, 31) < (v-1)(v-2)/6$ when $v \geq 16$, and the result follows. ■

Lemma 3: For $v \geq 16$, an $\mathrm{SQS}(v)$ can be reconstructed (up to isomorphism) from its block graph.

Proof: The blocks that contain a specified point form a clique of size $(v-1)(v-2)/6$, and the clique corresponds to the blocks of a derived $\mathrm{STS}(v-1)$. By Lemma 2, other types of cliques cannot be this large, so an $\mathrm{SQS}(v)$ can be reconstructed from its block graph by finding maximum cliques and identifying them with points. ■

We have now made all preparations for the main result.

Theorem 3: An extended 1-perfect code can be reconstructed (up to equivalence) from its minimum distance graph.

Proof: For lengths $n \leq 8$ the claim is trivial as these codes are unique, so we assume that $n \geq 16$.

Identify an arbitrary vertex with the all-zero codeword $\mathbf{0}$. By Lemma 1 we can construct the block graph of the neighborhood SQS of $\mathbf{0}$, and by Lemma 3 the neighborhood SQS itself. Now we have reconstructed all codewords with weight at most 4.

The codewords with weight 6 can be recognized by Lemma 1 and reconstructed as follows. Assume that $\mathbf{x}$ is such a codeword. If $x_i = 1$, then $\mathbf{x}$ has $\binom{5}{2} = 10$ neighbors $\mathbf{y}$ with $y_i = 1$, $\mathrm{wt}(\mathbf{y}) = 4$; if $x_i = 0$, then an upper bound for the number of such neighbors is given by the maximum size of a code of length 6, constant weight 3, and minimum distance 4, which is 4.

We proceed with induction on the weight of codewords. Assume that we have reconstructed all codewords with weight at most w, $w \geq 6$, and let $\mathbf{x}$ be a codeword with weight w.

For each coordinate r there is a set $\{i, j, k\} \subset \mathrm{supp}(\mathbf{x})$ such that $\{i, j, k, r\}$ is not a block of the neighborhood SQS of $\mathbf{x}$. Accordingly, $\mathbf{x}$ has three distinct neighbors $\mathbf{v}, \mathbf{y}, \mathbf{z}$ such that $\{r, i, j\} \subset \mathrm{supp}(\mathbf{x} - \mathbf{v})$, $\{r, i, k\} \subset \mathrm{supp}(\mathbf{x} - \mathbf{y})$, and $\{r, j, k\} \subset \mathrm{supp}(\mathbf{x} - \mathbf{z})$. Each of $\mathbf{v}, \mathbf{y}, \mathbf{z}$ has weight at most w, and hence those codewords are known. Furthermore,

$$\{r\} = \mathrm{supp}(\mathbf{x} - \mathbf{v}) \cap \mathrm{supp}(\mathbf{x} - \mathbf{y}) \cap \mathrm{supp}(\mathbf{x} - \mathbf{z}). \quad (1)$$

Consider the block graph of the neighborhood SQS of $\mathbf{x}$, and the maximum cliques from Lemma 3. Using (1) we can recognize the clique corresponding to the coordinate r. Now we know which neighbors of $\mathbf{x}$ differ from $\mathbf{x}$ in that coordinate. By repeating this for every r we can reconstruct the codewords corresponding to the neighbors of $\mathbf{x}$, and the result follows as each codeword $\mathbf{y}$ that is not the all-one word has a neighbor of weight $\mathrm{wt}(\mathbf{y}) - 2$. ■

Corollary 1: Weakly isometric extended 1-perfect codes are equivalent.

IV. Reconstructing 1-Perfect Codes

We will handle the problem of reconstructing a 1-perfect code from its minimum distance graph by reducing it to the problem of reconstructing an extended 1-perfect code from its minimum distance graph.

Lemma 4: The codewords with Hamming distance 4 can be recognized from the minimum distance graph of a 1-perfect code.

Proof: If codewords $\mathbf{x}, \mathbf{y}$ have Hamming distance 4, then their neighborhoods intersect in $\binom{4}{2} = 6$ vertices, since for any two coordinates of $\mathrm{supp}(\mathbf{x} + \mathbf{y})$ there is one neighbor of $\mathbf{x}$ which differs from $\mathbf{x}$ in those coordinates.

If the codewords are at distance 6, size of the intersection of their neighborhoods is at most 4 (attained by a Pasch configuration), and for other distances the neighborhoods do not intersect. ■

Theorem 4: A 1-perfect code can be reconstructed (up to equivalence) from its minimum distance graph.

Proof: Add new edges between codewords with Hamming distance 4 (Lemma 4). This gives the minimum distance graph for the extended code (obtained by adding a parity coordinate). Using Theorem 3 we can reconstruct the extended code. All codewords connected by new edges in the first step of the proof differ in the parity coordinate, which can thereby be detected. By puncturing in the parity coordinate we get the 1-perfect code. ■

Corollary 2: Weakly isometric 1-perfect codes are equivalent.

V. Automorphism Groups

The fact that the automorphism group of a 1-perfect code is isomorphic to the automorphism group of its minimum distance graph (for lengths $n \geq 15$) follow implicitly from [2], [3], [4], and the analogous result for extended 1-perfect codes (for lengths $n \geq 256$) from [5] combined with Theorem 1. The current study enables direct and concise proofs of these facts (expanded to lengths $n \geq 16$ for extended codes).

Theorem 5: The automorphism group of an extended 1-perfect code of length $n \geq 16$ is isomorphic to that of its minimum distance graph.

Proof: The automorphisms of the code can be mapped to automorphisms of the graph in the obvious fashion. Using the construction of Theorem 3, this homomorphism can be inverted; more specifically, we get an automorphism of the code by checking how $\alpha \in \mathrm{Aut}(G)$ maps the codeword $\mathbf{0}$ and the cliques used in the construction. ■

The result for 1-perfect codes now follows easily.

Theorem 6: The automorphism group of a 1-perfect code of length $n \geq 15$ is isomorphic to that of its minimum distance graph.

Proof: We use the construction from Theorem 4. Assume that extending a 1-perfect code C with a parity coordinate yields the code C'. Now $\mathrm{Aut}(C)$ is the subgroup of $\mathrm{Aut}(C')$ that stabilizes the parity coordinate. Similarly, if G is the minimum distance graph of C and G' the graph constructed in Theorem 4, $\mathrm{Aut}(G)$ is the subgroup of $\mathrm{Aut}(G')$ that stabilizes the new edges setwise. By Theorem 5 these subgroups are isomorphic, and hence $\mathrm{Aut}(C) \cong \mathrm{Aut}(G)$ as well. ■

VI. Conclusions

The result that 1-perfect and extended 1-perfect codes can be reconstructed from their minimum distance graphs is not only of theoretical interest but also has practical implications. Several methods have been used for deciding equivalence of (extended) 1-perfect codes [1], [9], [10]—the most straightforward method of representing the codes as graphs and deciding isomorphism of these graphs is rather inefficient [10]. The results obtained imply that this problem reduces to determining whether their minimum distance graphs are isomorphic.

References

[1] K. T. Phelps and M. LeVan, “Switching equivalence classes of perfect codes,” *Des. Codes Cryptogr.*, vol. 16, pp. 179–184, 1999.

[2] S. V. Avgustinovich, “Perfect binary $(n, 3)$ codes: The structure of graphs of minimum distances,” *Discrete Appl. Math.*, vol. 114, pp. 9–11, 2001.

[3] S. V. Avgustinovich, “On isometry of close-packed binary codes,” *Discrete analysis (Russian)*, (in Russian), Izdat. Ross. Akad. Nauk Sibirsk. Otdel. Inst. Mat., Novosibirsk, pp. 3–5, 1994. English translation in *Siberian Adv. Math.*, vol. 5, no. 3, pp. 1–4, 1995.

[4] F. I. Solov’eva, S. V. Avgustinovich, T. Honold, and W. Heise, “On the extendability of code isometries,” *J. Geom.*, vol. 61, pp. 3–16, 1998.

[5] S. V. Avgustinovich and F. I. Solov'eva, "On the metrical rigidity of binary codes," (in Russian), *Problemy Peredachi Informatsii*, vol. 39, no. 2, pp. 23–28, 2003. English translation in *Probl. Inf. Transm.*, vol. 39, pp. 178–183, 2003.

[6] D. A. Spielman, "Faster isomorphism testing of strongly regular graphs," in *Proc. 28th Annual ACM Symposium on the Theory of Computing* (Philadelphia, Pennsylvania), May 22–24, 1996, pp. 576–584.

[7] P. Kaski and P. R. J. Östergård, "The Steiner triple systems of order 19," *Math. Comp.*, vol. 73, pp. 2075–2092, 2004.

[8] B. M. I. Rands, "An extension of the Erdős, Ko, Rado theorem to t-designs," *J. Combin. Theory Ser. A*, vol. 32, pp. 391–395, 1982.

[9] P. R. J. Östergård and O. Pottonen, "The perfect binary one-error-correcting codes of length 15: Part I—Classification," submitted for publication. Preprint at arXiv:0806.2513v1.

[10] K. T. Phelps, "An enumeration of 1-perfect binary codes," *Australas. J. Combin.*, vol. 21, pp. 287–298, 2000.